



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/606,144

06/25/2003

Vincent J. Zimmer

20002/16809

3965

34431

7590

08/23/2007

HANLEY, FLIGHT & ZIMMERMAN, LLC

150 S. WACKER DRIVE

SUITE 2100

CHICAGO, IL 60606

EXAMINER

LASHLEY, LAUREL L

ART UNIT

PAPER NUMBER

2132

MAIL DATE

DELIVERY MODE

08/23/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

SD

Office Action Summary

Application No.

10/606,144

Applicant(s)

ZIMMER ET AL.

Examiner

Laurel Lashley

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 June 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|--|
| <p>1) <input type="checkbox"/> Notice of References Cited (PTO-892)</p> <p>2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)</p> <p>3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____</p> | <p>4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____</p> <p>5) <input type="checkbox"/> Notice of Informal Patent Application</p> <p>6) <input type="checkbox"/> Other: _____</p> |
|--|--|

DETAILED ACTION

Response to Amendment

1. No amendments were filed on 06/07/07. Claims 1 – 28 are still pending.

Response to Arguments

2. Applicant's arguments filed 06/07/07 have been fully considered but they are not persuasive.
3. It is Applicant's assertion that there is no "apparent reasoning" or "rational underpinning" to combine known elements which are required to render claim 1 obvious. The Examiner respectfully disagrees.

In response to applicant's argument that with regard to claim 1, there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Patel is concerned with securing communication channels in a pre-boot state. This is achieved through controlled access to storage areas. Chou is concerned with security securing a computer system by making it inoperable to unauthorized users. This is achieved through the security function stored in the BIOS. Zitlaw discloses selecting boot memory. England discloses a booting environment that enforces authorized user access via digital rights. Therefore it would be obvious to modify the password routing of Chou such that it would be digitally signed and authenticated as in England. Since the boot code of England would be used to validate the user in Chou. The motivation would be to improve the security of the reboot environment against unauthorized users. Furthermore it would be obvious

Art Unit: 2132

to limit availability of the memory management unit of Zitlaw to the memory areas of Patel since the memory management unit of Zitlaw is responsible for selecting boot memory space of Patel for authorized users. Therefore the motivation for combining England, Chou, Patel and Zitlaw would have been to protect password entry and authentication from unauthorized disclosure/access in a pre-boot environment..

It is Applicant's further assertion that "the references make it clear that reasoning for such a combination would not be apparent because the prior art counsels against the combination" of Zitlaw, Patel, Chou and England. Again the Examiner respectfully disagrees.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Applicant also contends that "claim 1 is not obvious because it incorporates new functionality into its elements that yields unexpected and fruitful results".

Applicant's arguments fail to comply with 37 CFR 1.111(b) because this argument amounts to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicant's presents similar arguments for claims 2 – 28 and are thus rejection on the basis of similar rationale. For at least these reasons the Examiner maintains the rejection of claims 1-28.

Claim Rejections - 35 USC § 103

Art Unit: 2132

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1 – 11, 23, 26 - 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. in US Patent No. 5892906 (hereinafter US '906) further in view of England et al in US Patent No. 6327652 (hereinafter US '652), Patel in US Patent No. 6327660 (hereinafter US '660) and Zitlaw et al. in US PGPub No. 20040128425 (hereinafter US PGPub '425).

5. For claim 1 similar claim 26, US '906 discloses:

A method of receiving a password, the method comprising:

receiving a password routine, (*see Abstract; column 3, lines 25 – 28; column 4, lines 1 – 4;*

column 5, lines 9 – 13: security function determines password authentication in BIOS routine)

storing the password routine, unavailability of data (*see column 7, lines 53 - 55*) and

executing the password routine in a pre-boot environment to receive the password (*see column 4, lines 1 -4*),

but does not expressly disclose the password routine being digitally signed using a private key, authenticating the password routine using a public key associated with the private key, or a first area of a memory device, the first area of the memory device being unavailable to a memory management unit, the memory device including a second area, the second area being available to the memory management unit.

England however does disclose the password routine being digitally signed using a private key (*see column 14, lines 60 – 61: boot code signed*), and

authenticating the password routine using a public key associated with the private key (*see column 14, lines 66 – 67: public key used to validate signature*) but does not expressly disclose

Art Unit: 2132

a first area of a memory device, the first area of the memory device being unavailable to a memory management unit, the memory device including a second area, the second area being available to the memory management unit.

Patel however does disclose a first area of a memory device, the first area of the memory device being unavailable and, the memory device including a second area, the second area being available (*see column 3, lines 35 – 39 and 47 - 48: first and second electronic systems equivalent to first and second memory areas; operational state (i.e. fully and not fully) is equivalent to availability state*) but does not expressly disclose the unavailability and availability to a memory management unit.

Zitlaw et al. however does expressly disclose a memory management unit (see page 2, [0008], lines 3 – 4; Figure 1B: memory controller).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the method of receiving a password routine of Chou et al. such that it would be digitally signed and authenticated as in England et al. to include a first and second memory areas (first and second electronic systems) of Patel such that it would limit the availability to the memory management unit as in Zitlaw et al. The motivation for doing so would have been to protect password entry and authentication from unauthorized disclosure/access in a pre-boot environment.

For claim 2, US '906 teaches:

A method as defined in claim 1, further comprising executing a non-trusted device driver in the pre-boot environment. (see column 3, lines 33 – 35 and 60 - 62)

For claim 3, US '906 teaches:

A method as defined in claim 2, wherein the non-trusted device driver is only executed if the

Art Unit: 2132

password matches a password stored (see column 4, lines 17 - 19) but does not expressly disclose storing the password in a first area of the memory device.

Patel however does disclose a first area of a memory device (*see column 3, lines 35 – 39 and 47 - 48: first electronic system*).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the method of receiving a password as in Chou et al. to include a first electronic system of Patel. The motivation for doing so would have been to provide a secure memory area to facilitate password authentication.

For claim 4, US '906 discloses a non-trusted device driver (*see column 3, lines 33 - 35*) but does not expressly disclose storing in the second area of the memory device.

Patel however does disclose a second area of the memory device (*see column 3, lines 35 – 39 and 47-48: second electronic system*).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the method of receiving a password of Chou et al. to include a second electronic system of Patel. The motivation for doing so would have been to provide a non-secure memory area to facilitate password entry.

For claim 5, US '906 discloses:

A method as defined in claim 1, wherein executing the password routine comprises executing the password routine using a processor in a secure mode, the secure mode being a hardware feature of the processor (*see column 3, lines 52 – 62: operating system not loaded*).

For claim 6, US '906 teaches:

A method as defined in claim 5, wherein the secure mode limits the use of input hardware. (*see column 3, lines 60 – 62; column 4, lines 18 -19: access dependent on match or mismatch*)

Art Unit: 2132

For claim 7, US '906 teaches:

A method as defined in claim 6, wherein the secure mode limits the use of output hardware.

(see column 3, lines 60 – 62; column 4, lines 18 -19: access dependent on match or mismatch)

For claim 8, US '906 teaches:

A method as defined in claim 1, wherein the password routine calls a trusted graphics routine, the trusted graphics routine being digitally signed. *(see column 3, lines 35 – 36; column 6, lines 63-64: private/public key pair; column 7, lines 52 – 60: prompt)*

For claim 9, US '906 discloses:

A method as defined in claim 8, wherein the trusted graphics routine calls a trusted display driver, the trusted display driver being digitally signed. *(see column 3, lines 35 – 36: monitor; column 6, lines 63-64: private/public key pair)*

For claim 10, US '906 discloses:

A method as defined in claim 1, wherein the password routine calls a trusted keyboard driver, the trusted keyboard driver being digitally signed. *(see column 3, lines 35 – 36: monitor; column 6, lines 63 - 64: private/public key pair)*

For claim 11, US '906 discloses:

A method as defined in claim 1, wherein the password comprises a basic input output system (BIOS) password. *(see column 1, line 57: BIOS device)*

For claim 23, US '906 discloses:

An apparatus as defined in claim 22, wherein the keyboard driver, the display driver and the graphics routine each authenticated using a digital signature *(see column 3, lines 35 – 36; column 6, lines 63 – 64; column 7, lines 52 - 60)* but does not expressly disclose the password collection routine authenticated using a digital signature.

Art Unit: 2132

England however does disclose the password collection routine authenticated using a digital signature (see *column 14, lines 66 – 67: public key used to validate signature*).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the apparatus as defined in claim 22, such that the password collection routine of Chou et al. would be authenticated using a digital signature as in England et al. The motivation for doing so would have been to protect password entry and authentication from unauthorized disclosure/access in a pre-boot environment.

For claim 27, US '906 teaches:

A machine readable medium as defined in claim 26, wherein the instructions are structured to cause the machine to executing a non-trusted software routine in the pre-boot environment, the non-trusted software routine being stored (see *column 3, lines 33 - 35*) but does not expressly disclose a second area of the memory device.

Patel however does disclose a second area of the memory device (see *column 3, lines 35 – 39: second electronic system*).

At the time of the invention it would have been obvious to a person skilled in the art to modify the machine readable medium of Chou et al. to include a second area of a memory device as in Patel. The motivation for doing so would have been to provide a non-secure memory area to facilitate password entry.

For claim 28, US '906 teaches:

A machine readable medium as defined in claim 27, wherein the non-trusted software routine comprises a legacy driver. (see *column 3, line 45*)

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2132

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 12 – 22, 24 - 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. in US Patent No. 5892906 (hereinafter US '906) further in view of Patel in US Patent No. 6327660 (hereinafter US '660) and Zitlaw et al. in US PGPub No. 20040128425 (hereinafter US PGPub '425).

7. For claim 12 and similar claim 22, US '906 teaches:

An apparatus to execute a trusted software program in a pre-boot environment, the apparatus comprising: (see Abstract; Figure 1 and associated text)

a memory device (see column 3, lines 31 - 32) and

a processor operatively coupled to the memory device, the processor to execute the trusted software program in the pre-boot environment (see Figure 1: item 10 and associated text)

but does not expressly disclose a first area of a memory device, the first area of the memory device being unavailable to a memory management unit, the memory device including a second area, the second area being available to the memory management unit.

Patel however does disclose a first area of a memory device, the first area of the memory device being unavailable and the memory device including a second area, the second area being available (see column 3, lines 35 – 39 and 47 – 48) but does not expressly disclose a memory management unit.

Zitlaw et al. however does expressly disclose a memory management unit (see page 2, [0008], lines 3 – 4; Figure 1B: memory controller).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the method of receiving a password of Chou et al. to include a first and second memory areas (first and second electronic systems) of Patel such that it would be limit the

Art Unit: 2132

availability to the memory management unit as in Zitlaw et al. The motivation for doing so would have been to protect password entry and authentication from unauthorized disclosure/access in a pre-boot environment.

For claim 13, US '906 discloses:

An apparatus as defined in claim 12, further comprising a non-trusted software program (see column 3, lines 33 - 35) but does not disclose a second memory portion.

Patel however does disclose a second memory portion (*see column 3, lines 35 – 39: second electronic system*).

At the time of the invention it would have been obvious to a person skilled in the art to modify the apparatus of Chou et al. to include a second memory location as in Patel. The motivation for doing so would have been to provide a non-secure memory area to facilitate password entry.

For claim 14, US '906 teaches:

An apparatus as defined in claim 13, wherein the processor executes the non-trusted software program in the pre-boot environment. (see column 3, lines 33 – 35 and 60 - 62)

For claim 15, US '906 teaches:

An apparatus as defined in claim 12, wherein the trusted software program comprises a hardware driver. (see Figure 1, item 10)

For claim 16, US '906 discloses:

An apparatus as defined in claim 15, wherein the hardware driver comprises a keyboard driver. (see column 3, lines 35 – 36: keyboard)

For claim 17, US '906 discloses:

An apparatus as defined in claim 15, wherein the hardware driver comprises a display driver. (see column 3, lines 35 – 36: monitor)

Art Unit: 2132

For claim 18, US '906 teaches:

An apparatus as defined in claim 12, wherein the trusted software program comprises a graphical user interface display routine. (see column 3, lines 35 – 36; column 7, lines 52 – 60: "prompt")

For claim 19, US '906 teaches:

An apparatus as defined in claim 12, wherein the trusted software program comprises a password collection routine. (see Abstract; Figure 1 and column 4, lines 1 - 5: security routine)

For claim 20, and similar claim 24 US '906 discloses:

An apparatus as defined in claim 12, wherein the processor includes a secure mode that limits the use of input hardware and output hardware connected to the processor. (see column 3, lines 60-62: access dependent on match or mismatch)

For claim 21, US '906 teaches:

An apparatus as defined in claim 20, wherein the processor executes the trusted software program in the pre-boot environment while the processor is in the secure mode. (see column 3, lines 52 -62)

For claim 25, US '906 discloses:

An apparatus as defined in claim 24, wherein the processor executes the keyboard driver, the display driver, the graphics routine, and the password collection routine in the pre-boot environment while the processor is in the secure mode. (see column 3, lines 35 – 36 and 52 – 62; column 7, lines 52 - 60)

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2132

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132

Art Unit: 2132

 17 August 2007



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100